Specialist Care Team

What is GDPR?

GDPR is a modification to the Data Protection Act and it comes into force on 25 May 2018. Under the legislation, we will continue to hold data securely on clients and employees. This document gives a brief overview on how we are in line with the regulations.

Updated 14th May 2018

Document owner:	**Anthony Murray**

What is GDPR?

Social care organisations hold a significant amount of personal information relating to individuals, whether they be employees, people who need care and support or other customers or suppliers. A proportion of that data is likely to constitute sensitive personal data or “special categories of data” (including, for example, medical records, religious beliefs or ethnic origin).

From 25 May 2018, all organisations that process personal data are required to comply the General Data Protection Regulation (GDPR), which is European-wide legislation. It is a regulation to strengthen and unify data protection for all individuals within the EU.

To implement GDPR, the UK government approved The Data Protection Act 2018 on 23 May 2018, which sets new standards for protecting general data, giving people more control over use of their data, and providing them with new rights to move or delete personal data.

What is Personal Data?

Personal data is any information that relates to a living individual. It does not include personal information about somebody who has died. The definition of personal data is wider under GDPR than under the Data Protection Act and includes specific identifiers, such as a person's name and email address, as well as factors about a person, such as their physical appearance, physiological or mental state, their financial status or social identity. It could, therefore, include opinions you give about a person in their care records or care plan, and will certainly include a person's medical and health records. The definition also includes photographs and CCTV footage, as well as location data.

Special categories of data

"Special categories of data" are a type of personal data, and have broadly the same meaning as "sensitive personal data" under the Data Protection Act. They include types of data that are thought to be of a more sensitive nature, such as information about a person's medical history or health, their race or ethnic origin, their religious or political views and their sexual orientation. The definition also includes genetic data and biometric data. As a social care provider, Specialist Care Team is entitled to process Special Categories of Data.

The GDPR Key Principles are:

1. Processing should be lawful, fair and transparent

Data subjects should have a clear understanding of what personal data is being processed about them and why it is being processed. Any communication with the data subject about their personal data should be easily accessible, easy to understand and written in plain and clear language.

GDPR requires organisations to provide certain information to the data subject when the personal data is collected either directly from the data subject or from another source. The information may be provided to the data subject as part of a fair processing notice.

2. Personal data shall be collected for specified, explicit and legitimate purposes

Personal data should be collected for a specific purpose and the data subject should know what that purpose is. If an organisation wishes to use personal data for another purpose, it will need to get separate consent from the data subject for that particular purpose, or determine whether another ground

(such as legitimate interest or the processing of special categories of data for the provision of health and social care services) applies.

3. Personal data must be adequate, relevant and limited to what is necessary

Organisations should only process the personal data they need to process to achieve the purpose for which it was collected.

For example, diversity questionnaires are often completed on an anonymous basis so that the information in the questionnaires is not personal data – an organisation is unlikely to need to know a person's racial or ethnic origin or religious beliefs to be able to employ them or provide them with services. Organisations, staff and carers should have access to relevant health and medical records only, particularly given the volume of special categories of data contained within those documents.

4. Personal data shall be accurate and kept up to date

We have processes in place to ensure that personal data we process is accurate and up to date. For example, if a person's contact information changes, it should be updated as soon as possible and the previous, now inaccurate contact information will be deleted or removed. The same principle applies to personal data contained within care records – it will be regularly reviewed on a monthly basis and updated.

5. Personal data shall be kept for no longer than is necessary

GDPR requires personal data to be deleted or destroyed when it is no longer needed by the organisation. Alternatively, the personal data could be anonymised or otherwise modified so that it no longer relates to an individual. *There may be statutory or sector-specific reasons why personal data should be retained beyond the period for which the organisation needs it. For example, organisations are required to keep Right to Work documentation for 2 years beyond the termination of a person's employment. Contracts should be kept for 6 years and Deeds for 12 years in case a claim arises.*

6. There must be appropriate security in place in respect of the personal data

We have a number of security measures to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. For example, all digital documents are password protected and hard copies are stored in locked cabinets with restricted access. When using portable media, ie USB sticks they are immediately wiped once data has been transferred.

What have we done to comply with GDPR?

- We have appointed Anthony Murray as our Data Protection Officer. He will oversee the policy for Specialist Care Team and Clover House.
- We have determined the purposes and means for which personal data is processed. For example, when we are passed data we will decide how to use that data – for example, we will use medical records to understand which medicines need to be administered and to understand behavioural issues, and we will use phone numbers for next of kin to contact them in the event of an emergency.
- We have assessed the systems and processes that we use. We are satisfied that all systems are secure.

- Gaining Consent: We do not need to gain consent for the processing of personal data for service users and employees because we have a legitimate interest in processing this data. We will be unable to deliver our care service, for example, without processing data on the service user.
- To ensure we are compliant, we have distributed a fair processing notice to all employees and service users to make them aware that we are compliant with GDPR and to give them the opportunity to find out more information.